Sub D1

What Is claimed Is

~~CLAIMS~~

1. A method for executing secure data transfer between a communication device ~~(1)~~ and an application server ~~(5)~~, wherein data are transferred over a network ~~(2, 3)~~ between the application server ~~(5)~~ and the communication device ~~(1) (301, 302, 401, 402)~~, comprising ~~characterised by~~

sending an agreement proposal for a secure transaction of data from the server ~~(5)~~ to a security adapter ~~(6)~~ connected to the network ~~(2, 3) (303, 304, 305, 306, 403, 404)~~,

creating and sending a message from the security adapter ~~(6)~~ to the communication device ~~(1)~~ in order to activate a signing application ~~(307, 308, 309, 310, 405, 406, 407, 408)~~,

the signing application signing the data to be send ~~(311, 312, 409, 410)~~,

sending the signed data from the communication device ~~(1)~~ to the security adapter ~~(6) (313, 411)~~,

verifying the signature ~~(314, 412)~~ for the data, and

sending the verified signed data to the server for execution of the transaction ~~(315, 413)~~.

2. A method according to claim 1, ~~characterised in that~~ wherein information browsing on the server ~~(5)~~ is initiated from either the application server ~~(5)~~ or the communication device ~~(1)~~, wherein data are transferred over the network ~~(2, 3)~~ between the application server ~~(5)~~ and the communication device ~~(1) (301, 302, 401, 402)~~.

3. A method according to claim 1 ~~or 2, characterised~~ , comprising by, before the step of sending an agreement proposal, the further step of:

sending a request requiring a secure transaction of data, either from the communication device ~~(1)~~ to the application server ~~(5) (303, 403)~~, or from the application server ~~(5)~~ to the communication device ~~(1)~~.

4. A method according to claim 1 ~~any of the preceding claims~~, wherein ~~characterised in that~~ the step of sending a message from the security adapter ~~(6)~~ to the communication device ~~(1)~~ in order to activate a signing application further comprises the steps of:

entering details of the transaction to be secured and a sign request into at least one message ~~(308,406)~~,

sending the at least one message from the security adapter ~~(6)~~ to a smart card in the communication device ~~(1)~~ for activating the signing application ~~(309,407)~~,

displaying the details of the transaction and a prompt for an accept on the communication device ~~(1)~~ ~~(310,408)~~.

Sub D1

5. A method according to claim 1 ~~any of the preceding claims~~, wherein ~~characterised in that~~ the step of signing the data further comprises the step of:

accepting the transaction ~~(311,409)~~, the signing application signing the data to be send with a secret/private key by using an algorithm ~~(312,410)~~.

6. A method according to claim 1 ~~any of the preceding claims~~, wherein ~~characterised in that~~ the step of sending an agreement proposal comprises the further step of:

sending the agreement proposal for the secure transaction from the server ~~(5)~~ to the communication device ~~(1)~~ ~~(304)~~ for acceptance ~~(305)~~ before the agreement proposal is send to the security adapter ~~(6)~~ ~~(306)~~.

7. A method according to claim 4 ~~any of the claims 4-6, characterised~~ wherein in that the smart card is a SIM card (subscriber identity module), the data transfer protocol is the WAP (Wireless Application Protocol), the signing application is a SAT (SIM Application Toolkit) application, the communica-

tion application is a WAP application, and the message is at least an SMS or USSD packet.

wherein 8. A method according to claim 7, ~~characterised in that~~ the WAP application in the communication device is suspended or terminated when the SAT application is activated (~~307, 405)~~.

Sub D1

9. A system for executing secure data transfer between a communication device ~~(1)~~ and an application server ~~(5)~~ over a wireless network ~~(2, 3)~~, comprising ~~characterised by~~ a security adapter ~~(6)~~ connected to the network ~~(2, 3)~~ for monitoring the data transfer between the communication device ~~(1)~~ and the application server ~~(5)~~, wherein

said server ~~(5)~~ is adapted to send an agreement proposal for a secure transaction of data to the security adapter ~~(6)~~,

said security adapter ~~(6)~~ is adapted to receive said agreement proposal for a secure transaction from the server ~~(5)~~, and create and send a message to the communication device ~~(1)~~ for activating a signing application,

said communication device ~~(1)~~ is adapted to sign the data, and send the signed data to the security adapter ~~(6)~~,

said security adapter ~~(6)~~ is adapted to receive, and send the signed data for verification and then send the verified signed data to the application server ~~(5)~~ for execution of the transaction.

wherein 10. A system according to claim 9, ~~characterised in that~~ said communication device ~~(1)~~ comprises a secret/private key, an algorithm for signing of data, and a signing application for handling a signing dialogue and the signing of data.

11. A system according to claim 10, ~~characterised in that~~ wherein said secret/ private key, said algorithm, and said signing application is stored on a smart card such as a SIM card (subscriber identity module), the data transfer protocol is the WAP (Wireless Application Protocol), the signing application is a SAT (SIM Application Toolkit) application, and the message is at least an SMS or USSD packet.

12. A system according to claim 9 ~~any of the claims 9-11~~, ~~characterised in that~~ wherein said network comprises a mobile telephone network ~~(2)~~ for connection to the communication device ~~(1)~~, the Internet ~~(3)~~ for the connection to the application server ~~(5)~~, and a WAP gateway ~~(4)~~ connecting the mobile telephone network ~~(2)~~ to the Internet ~~(3)~~.

13. A system according to claim 12, ~~characterised in that~~ wherein said security adapter ~~(6)~~ is connected to the WAP gateway ~~(4)~~.

14. A system according to ~~any of the~~ claim~~s~~ 9~~-12~~, ~~characterised in that~~ said security adapter ~~(6)~~ is connected to the application server ~~(5)~~.

15. A system according to ~~any of the~~ claim~~s~~ 9~~-14~~, ~~characterised in that~~ wherein said communication device is a mobile phone ~~(1)~~ or a portable computer having transmitting /receiving capability.

16. A system according to claim 15, ~~characterised in that~~ wherein the mobile phone comprises means for displaying a particular icon, character, font, or colour connected to certain applications or the operating system in the phone, wherein the user can be assured that he is really communicating directly with the security application.

Sub D17

17. A security adapter for connection to a wirless network ~~(2,3)~~ for monitoring the data transfer between a communication device ~~(1)~~ and an application server ~~(5)~~ connected to the network, comprising ~~characterised by~~

means for receiving an agreement proposal for a secure transaction from the communication device (1),

means for creating and sending a message to the communication device (1) in order to activate a signing application,

means for receiving signed data send from the communication device (1), and

means for sending the signed data for verification and then to the application server (5) for execution of the transaction.

18. A computer program product directly loadable into the internal memory of a security adapter ~~(6)~~ with digital computer capabilities, comprising ~~characterised by~~ comprising software code portions for performing the steps of:

receiving an agreement proposal for a secure transaction from a communication device ~~(1)~~,

creating and sending a message to the communication device ~~(1)~~ in order to activate a signing application,

receiving signed data send from the communication device ~~(1)~~, and

sending the signed data for verification and then to an application server ~~(5)~~ for execution of the transaction.

19. A computer program element comprising computer program code means to make a security adapter ~~(6)~~ with digital computer capabilities execute the steps of:

receiving an agreement proposal for a secure transaction from a communication device ~~(1)~~,

creating and sending a message to the communication device ~~(1)~~ in order to activate a signing application, D'and

B

receiving signed data send from the communication device ~~(1)~~, and

B

sending the signed data for verification and then to an application server ~~(5)~~ for execution of the transaction.

20. A computer program element as claimed in claim 19 embodied on a computer readable medium.